CHAPTER 6

ADP INTERNAL CONTROL TECHNIQUES

A. GENERAL

1. This chapter contains detailed ADP internal control techniques to be considered when developing or significantly modifying computer systems or applications. The section is divided among the three components of ADP internal control:

- Management Controls.
- Operations Controls.
- Application Controls.

2* The specific techniques are listed by element within these three areas. While the techniques in these areas generally apply to microcomputers, this Guideline separately presents internal control techniques specifically applicable to microcomputers; these techniques are presented in sect ion D of this chapter. Users of microcomputers should refer to the techniques presented in section D. as well as those listed under Management Controls, Operations Controls, and Applicat ion Controls to ensure control over microcomputer operations.

3. It should be emphasized that the control techniques are listed only for consideration. It is left to the discretion of the reader to determine which techniques to apply based upon unique organizational and environmental characteristics and the related formulation of specific control objectives.

B. MANAGEMENT CONTROLS . Like any other resource, ADP needs to be properly managed to take full advantage of its capabilities. Managers should exercise sufficient control over the ADP function to determine how well it operates, where improvements are needed, and what capabilities will be needed in the future. To accomplish these objectives, control techniques that contribute to the effectiveness of the overall ADP program management should be considered as an element of the following areas:

- ADP Planning.
- Policies. T. Standards and Procedures.
- Organizational Controls.
- Internal Audit.

1. ADP Planning. The activities of the ADP organization

ADP's objectives, both long- and short-range, should be consistent with those of the organization. The DoD process that applies in this area is Life-Cycle Management (LCM) and uses the principles set forth in DoD Directive 7920.1 and DoD Instruction 7920.2 (references (n) and (o)). The following techniques should be considered by ADP management to assure that ADP activities are properly planned.

a. An ADP management process that considers inputs from the various involved organizations, including major user departments and program areas, should be applied to:

(1) formulate policies for ADP systems;

(2) justify the need for new computer equipment; and

(3) assure that new equipment is acquired in the most economical and expeditious manner;

b. The facility should have formalized short- and long-range ADP plans;

c. The planning process should establish and document mission requirements, strategy, and overall system goals and objectives;

d. The ADP planning process should establish and document individual responsibility for specific actions to be undertaken;

e. . ADP planning should be related to budgeting for financial, personnel, and system resources and to comparing and selecting among system alternatives based upon quantified life cycle cost, benefit, and risk projections;

f. The planning process should measure and compare actual accomplishments with expected performance throughout the system life-cycle;

g. Management should be informed of the status" of planned actions through regular progress reports;

h. Regular internal audit review and reporting should be conducted regarding completed and proposed planning decisions in relation to mission requirements;

i. The ADP planning process should take into account relevant computer security requirements affecting the scope of ADP activity.

j. The ADP planning process should take into account approved agency records disposition schedules.

2. Policies, Standards and Procedures. Policies, standards, and procedures should exist and serve as the basis for management planning, control and evaluation. The following techniques should be considered to accomplish this objective:

a. The procedures for the ADP management process should be formally established;

b. All appropriate organizational components of the site involved with ADP systems should be defined and clearly assigned their respective areas of functional responsibility;

c. ADP resources acquisition, system design, programming, and operating standards should be established, coordinated and communicated to all affected personnel;

d. Policies to assist decision-makers in selecting among system development and operations alternatives (e.g., contracting versus in-house, shared versus separate facilities, purchase versus lease) should be established;

e. Procedures and responsibilities should be established for ensuring that, as applicable, OMB and GSA are apprised of ADP system initiatives;

f. Comprehensive ADP cost accounting procedures in accordance with-GAO's Federal Government Accounting Pamphlet No. 4, "Guidelines for Accounting for Automatic Data Processing costs," and OMB Circular A-130, Appendix II, "Cost Accounting, Cost Recovery and Inter-Agency Sharing of Data Processing Facilities" (reference (e)) should be established as appropriate;

g. Rigorous ADP budgeting procedures should be implemented to ensure that all significant ADP-related initiatives, expenditures, and reprogramming are clearly highlighted, whether or not they fall within budget decision units or are spread over multiple decision units;

h. Rigorous project control and performance measurement techniques (e.g., PERT, CPM) and progress reporting should be required based upon actual cost and work-year expenditures, deliverables provided, and milestones achieved (rather than upon subjective percent of completion estimates);

i. Policy and procedures should be established to comply with systems security, privacy, and freedom of' information requirements;

j. Procedures describing the manner and responsibility for performance between users and ADP should be-established, coordinated, and communicated to all affected organizations.

3. Organizational Controls. Effective controls need to be established over the data processing operation because of the concentration of functions brought about by the computer. The organizational structure should provide assurance that assets are safeguarded and that information is produced reliably. A key organizational control is an adequate separation of duties, which includes:

Separating the data processing functions from other agency functions;

Separating different data processing functions within the data processing organization;

Providing for separation of duties within user departments.

Personnel capabilities need to be considered in determining
* which techniques are appropriate for establishing effective organizational controls. The following techniques should be considered to implement effective organizational controls over the ADP function:

a. The ADP function should be placed sufficiently high in the organization to ensure its independence from other site operations;

b. All ADP employees should be prohibited from having authority or duties in any other organization without management approval;

c. Major organizational units within ADP should be described and their responsibilities delineated and documented;

d. Where practical, the following functions should be performed by a different individual or group:

Systems analysis.

- Application programming.
- Acceptance testing.
- Program change control.
- Data control.
- Production control and scheduling.
- Computer equipment operation.
- System software maintenance.
- Computer files maintenance.

- Source document origination.

- Source document conversion to machine-readable format.

e. . Transactions generally should originate and be authorized in an organization outside of ADP;

f. A direct line of responsibility should exist between every subordinate and supervisor;

g. A personnel rotation plan should be in effect within the different functional areas in the ADP organization;

h. ADP personnel should be required to take regularly scheduled vacations;

i. Absentee and turnover rates in the ADP organization should be monitored for potential personnel problems;

j. ADP position descriptions should be in writing, be clear in delineating authority and responsibil.ity, be kept current, be accompanied by definitions of technical skills needed, and be usable as a basis for performance ’evaluation;

k. Personnel recruiting and promotion practices should be based on objective criteria and should consider education, experience, and security risks relevant to the job requirements and to the degree of responsibility;

1. Before being hired, ADP personnel should be subjected to preemployment checks;

m. When hired, employees should be provided with an orientation of internal controls and security and with ongoing training to maintain their technical knowledge, skills, and abilities;

n. Training programs should exist to maintain and build skills, knowledge, and ability in systems technology, internal control, and ADP security requirements;

o. Employee performance should be evaluated on a regular basis, and any negative performance should be appropriately addressed.

4. Internal’Audit. The Component’s internal audit staff should be responsible for assuring top management that systems are developed in accordance with objectives, contain the needed internal controls to produce consistently reliable results, and operate in conformance with management standards and approved design specifications.

a. The . internal auditors charter should allow the conduct of independent reviews and the reporting of findings and recommendations to the site's management;

b. The responsibility of the internal audit function in relation to ADP should be clearly documented;

c. Internal Audit should actively participate in reviewing the development of new systems or applications and the significant modification of existing systems;

d. During system planning and development, internal audit should ensure that the system carries out prescribed management policies;

e. Internal audit should review general controls in data processing systems to determine that controls have been designed according to management direction and legal requirements and that these controls are operating effectively to provide reliability of, and security over, the data being processed;

f. Internal audit should review application controls of computer-based systems to assess their reliability in processing data in a timely, accurate, and complete manner;

g. These control reviews should ascertain whether the systems conform to both organization and Federal standards;

h. Periodic audits should be designed to test both internal controls and reliability of processed data;

i. When appropriate, Internal audit should verify the information on output reports against related source documents.

C . OPERATIONS CONTROLS. Operations controls apply to all processing carried out within a computer installation and are independent of any specific application. Operations controls include:

- Data center operations controls;
- Security controls;
- System software controls;
- Hardware controls; and
- Distributed processing and network operation controls.

The effectiveness of these controls are of high importance in the ADP environment because weaknesses can affect all processed applications.

1. Data Center Operation Controls. Control procedures concerning data center operations should be established and followed to ensure accuracy and completeness of the information maintained and processed by the ADP facilities. These controls should be to prevent errors in data preparation and handling and aid in production scheduling, file updating, and output report preparation. Strong controls in specific key areas will help prevent or decrease the probability of inaccurate or fraudulent processing. Data center operations controls can be broken down into the following areas:

- Work Load Scheduling Controls.
- Malfunction Reporting and Preventive Maintenance Controls.
- User Billing/Charge-back Controls.

a. Work Load Scheduling Controls. Control procedures over work load scheduling and the inputting and outputting of data should be enacted and complied with. Certain production scheduling and input and/or output controls may be bypassed when remote job entry devices are used to schedule. However, a control group should monitor and manage these operations. The following control techniques should be considered to ensure that proper controls are being maintained over workload scheduling:

(1) A formal control group should be established within the data center to monitor both remote decentralized as well as centralized job entry;

(2) Formal input and/or output control procedures should be established and documented;

(3) All personnel should have a copy of a manual detailing required control procedures.;

(4) The control group should be responsible for recording and controlling the production data processed by the data processing organization;

(5) All totals should be balanced during and after applications processing, and all processing errors should be controlled by the control group;

(6) An authorization document or a transmittal sheet should be required to accompany all input transactions;

(7) All output reports should be visually scanned by the control group for general accuracy and completeness and be distributed according to a formal schedule;

(8) The control group should establish and document formal scheduling procedures, schedule production runs

and other workloads, and reschedule aborted or erroneous processing;

(9) A priority scheme of classes or priorities should be used for scheduling work;

(10) A schedule of all computer-based systems should exist and include a brief description of the function of each system, the date of approval, and an identification number;

(11) Source documents should be maintained for reference in a logical sequence for a suitable period of time;

(12) All characteristics of jobs (run time, data sets, access time, computer devices required, etc.) within the job stream should be defined and documented;

(13) The mix of on-line and batch jobs should be scheduled in order to promote efficient use of facilities and to meet user requirements;

(14) A systematic time-related flow of jobs through each work center should be established;

(1S) Users should be involved with workload scheduling, except in emergencies;

(16) Operators should not be involved with workload scheduling, except in emergencies;

(17) Rush or rerun jobs should be scheduled consistent with their priority ratings;

[18) Reasons for schedule delays should be identified by area of responsibility;

(19) Approximate elapsed time of delay should be recorded for each delay event;

(20) In on-line systems, response time statistics should be kept and monitored for significant fluctuations in response time;

(21) CPU utilization statistics should be monitored for both batch and on-line processing;

(22) Significant variances in performance should be followed up by the control group.

b. Malfunction Reporting and Preventive Maintenance Controls.

(1) Control procedures concerning malfunction reporting and preventive maintenance should be established and

followed. Malfunction reporting should ensure that errors and omissions resulting from hardware or software system crashes are reported. In addition, it should provide measures of the adequacy of the preventive maintenance, of the level of vendor maintenance provided, and of the failure rate of the system. Preventive maintenance should be performed according to established facility and vendor procedures.

(2) The following control techniques should be considered to ensure that, proper controls are being maintained over malfunc-tions reporting and preventive maintenance:

(a) Formal malfunction reporting procedures should be established and documented for the data processing installation;

(b) Operators and all other appropriate personnel should have access to a manual detailing these control procedures and certify in writing that they have reviewed and understood them;

(c) These logs should record start ups, errors, reruns, recoveries, shut downs, shift' changes, and maintenance occurrences;

(d) Log pages should be sequentially numbered;

(e) The computer system should automatically produce a log of all system operations;

(f) The console log should include the date, job name and number, program name and number, start and/or stop times, files used, record counts, and scheduled and unscheduled halts;

(g) Disposition notes should be entered on the console log showing corrective actions taken when unscheduled program halts occur;

(h) Job reruns should be recorded along with their reason on the console log;

(i) Console log pages should be sequentially numbered;

(j) Logs should be reviewed and signed at the end of each shift by a supervisor and filed as a permanent record;

(k) Logs should be independently examined to detect operator problem and unauthorized intervention;

(1) System crashes should be isolated and identified by cause;

(m) System reliability reports should include Mean Time Between Failures (MTBF) and Mean Time to Recovery (MTTR) statistics;

(n) System -performance records should be maintained;

(o) Formal preventive maintenance procedures should be established and documented for the data processing organization;

(p) Logs of the type and time of maintenance performed should be kept;

(q) A schedule for machine maintenance should be published and followed;

(r) Sensitive data should be removed from on-line storage devices before equipment is turned over to maintenance personnel;

(s) The production schedule should be flexible enough to accommodate prevent ive maintenance;

(t) Preventive maintenance should not be scheduled during peak load periods.

C. User Billing and Charge-back Controls.

(1) Control procedures over user billing and charge-back should be established and complied with. Controls should be designed to encourage appropriate usage of computer resources and fair treatment of users and their needs. All costs should be derived on a fair and equitable basis in accordance with management policy and procedures and with Federal guidelines.

(2) The following control techniques should be considered to ensure that proper controls are being maintained over user billing and charge-back procedures:

(a) Procedures for user billing and charge should be documented;

(b) Billing and charge-back agreements should exist between users and the data processing organization;

(c) The user billing charge-back procedures should be effectively tied into a job accounting system for the data processing resources;

(d) The user billing and charge-back procedures should be based on the number of transactions processed, on an artificial "computer accounting unit ," or some other equitable method;

(e) Adequate procedures should exist for determining the share of system development costs plus additional overhead items, such as lighting, space, and air conditioning, for billing users;

(f) Additions and replacements of hardware, software, etc. should be, justified on the basis of resource utilization and user needs;

(g) An equitable procedure should exist for charging reruns of productions jobs so that user errors are charged back to users, while data processing organization errors are absorbed by data processing;

(h) Current data processing organization costs should be consistent with budgeted costs;

(i) Periodic billing statements should be provided to user departments describing cost details and the billing algorithm used;

(j) Rates charged to users should encourage the use of data center resources in accordance with users' needs; differential rates for off-peak usage or the assignment of processing priorities for varying turnaround requirements should be used to encourage maximum usage of centralized computer facilities.

2. Security Controls. Control procedures concerning computer security should be enacted and followed to protect and safeguard ADP resources. The hardware, software, and data are all assets that should be managed properly and protected against theft, loss, unauthorized manipulation, fraudulent activities, and natural disasters. To minimize these risks, controls to limit access to the data center, decentralized hardware, system and application programs, system documentation, and outputs should be established. Site 'management should also establish and enforce strict procedures over maintenance, storage, and access to data storage media as well as preventive procedures that help protect critical files, programs, and system ' documentation from natural disasters. Security controls can be broken down into the following areas;

Administrative Controls;

Physical Controls;

Technical Controls;

Disaster Recovery Controls.

Control techniques that should be considered in each of these areas are presented in the following sections.

a. Administrative Controls. The following techniques should be considered to effectively administer the ADP security function.

(1) Responsibility for conducting risk analyses should be formally assigned.

(2) Responsibility should be assigned for computer security at each ADP facility;

(3) Individuals assigned responsibility for computer security should be given training and experience in both the computer and security areas;

(4) Risk analysis studies should measure vulnerability related to the potential for the following:

(a) Fraud or theft,

(b) Inadvertent error or improper disclosure of information,

(c) Financial loss,

[e) Harm to individuals or infringement on privacy rights,

(f) Loss of proprietary data and harm to organizational activities;

(5) A specific timetable for conducting risk analysis studies should be established, with the time between studies being commensurate with the sensitivity of the information processed;

(6] Risk analysis studies should be performed at least every 5 years;

(7) Procedures should require that a risk analysis be performed before the approval of design specifications for computer installations or whenever significant changes are made to the physical facility, hardware, or operating system software;

(8) Requirements should be established for conducting risk analysis for DoD government-owned, contractor-operated facilities and for Government-operated facilities;

(9) Plans should provide for assessing risks related to computer services provided by other agencies and those provided through commercial services;

(10) Employees utilizing ADP equipment and processing DoD data should be required to sign an agreement regarding their role and responsibility at the facility and in the ownership and use of data processing equipment and information within the data center;

(11) ersonnel security policies for screening employees and contractor and/or service personnel should be established and provide for levels of screening commensurate with the sensitivity of the position or function;

(12) When an employee is terminated, the employee should immediately be denied access to the data processing organization, any data, program listings, etc.; and all other employees should be informed of the employee's termination;

(13) Procedures should exist to handle a situation in which an employee' becomes a suspected security risk.

b. Physical Controls. In order to reduce the risk of erroneous or fraudulent activities, physical security controls should exist to protect ADP resources against unauthorized access. The following physical security control techniques should be considered to accomplish this objective:

(1) Written procedures should exist to define restrictions to computer room access;

(2) A reliable guard service or alarm system should exist to protect the computer center against illegal entry, vandalism, or sabotage;

(3) Access to the computer areas should be restricted to only authorized and appropriated personnel through the use of a passcard system, combination locks, security badges, or other appropriate secure means;

(4) Combinations on locks or similar devices should periodically be changed;

(5) Account codes, authorization codes, Passwords, etc. should be controlled to prevent unauthorized use;-

(6) Restricted entrances and emergency exits should be equipped with tamperproof automatic alarm systems that signal when doors are opened;

(7) Exterior walls, tape library walls, storage room walls, etc. should be of solid construction from floor to ceiling;

(8) Data processing personnel should be trained to challenge improperly identified visitors;

(9) Data processing personnel should be counseled to report all intentional or inadvertent cases of security intrusions of which they become aware;

. (10) Access to the computer area by custodial, electrical and other in-house maintenance personnel should be supervised and controlled;

(11) Vendor and support personnel should provide positive identification before they can be admitted to the computer area;

(12) At least two individuals should be present in the computer room at all times;

(13) A procedure should exist to restrict access to source documents and blank input forms to authorized employees;

(14) All critical forms, such as identification cards, negotiable instruments, and source documents, should be prenumbered for accountability, stored in a secure location and periodically accounted for;

(15) Procedures should exist to limit access to critical forms during their intermediate storage and transportation, such as dual custody and mail message carrier controls;

(16) A procedure should exist for joint authorization of releases from the storage areas, and the receipt of critical forms should be inventoried by two people at the time of delivery;

(17) Procedures should be established to control the issuance of critical forms for jobs scheduled for processing;

(18) Copies of critical outputs that need to be destroyed should be kept in a secure location until they can be destroyed;

(19) At least two people should be present when critical outputs are destroyed.

c. Technical Controls. Control procedures over system and file access should be established and followed. The use of system security software, as well as of a librarian function, will reduce the possibility of illegal system access and erroneous or fraudulent processing. The following techniques should be considered to ensure systems security:

(1) Separate security software should be used to provide control over the site's computer resource;

(2) The vendor or developer of the security software should provide a completely documented description of its design and operation;

(3) The security software should control access to terminals, remote job entry station, individual automated data files, application programs, and other system software;

(4) Security software functions should be adequately supported by proper manual procedures;

(S) The control functions performed by security software should not be able to be overridden or bypassed;

(6) The security software should provide an audit trail of all authorized uses and unauthorized attempted accesses of computer resources under control;

(7) the security software should control access to data in a different manner than access to other computer resources;

(8) The security software should be transparent to all application programs and to all other system software;

(9) A list of all personnel should exist and be periodically reviewed by supervisors detailing what computer resources the personnel have access to;

(10) On an on-line environment, there should be access security control based on the classification of file data and devices;

(11) The responsibility for issuing and storing disk packs, magnetic tapes, or other data storage media should be assigned to a librarian;

(12) The responsibility referenced in item 11, above, should be the librarian' s chief function;

(13) Library procedures should be documented;

(14) Access to the library should be limited to authorized personnel;

(15) A librarian should be on duty whenever the data center is being used;

(16) Sensitive files, such as security classifications or Privacy Act restrictions (reference (l)) ,

should be properly identified as such, and appropriately secured;

(17) To prevent release to unauthorized personnel, all data files should be logged in and out;

(18) All files should be expeditiously returned to the library after use;

(19) Disk packs and tape inventory records should be kept;

(20) External labeling procedures should be documented;

(21) External labels should be affixed to active disks and/or tapes;

(22) Work or scratch tapes should be kept in separate area of the library.

d. Disaster Avoidance and Recovery. Control procedures concerning disaster recovery should be established and followed. Controls should help prevent fire or other natural disasters from destroying hardware, critical files, programs and system documentation. If a disaster were to occur, a disaster recovery plan should be implemented to ensure the recapture of critical information. These control procedures need to be formally documented and periodically tested and updated. The following techniques should be considered to minimize the impact of unanticipated interruptions:

(1) Emergency procedures should be formally documented and distributed to all associated personnel;

(2) Procedures should include steps to be taken in the event of an actual or likely natural disaster by fire, water damage, etc., and intentional damage by sabotage, mob action, bomb threats, etc.;

(3) The computer center should be separated from adjacent areas by fire resistant partitions and/or walls, and noncombustible flooring, ceilings, furniture, carpets and draperies should be used;

(4) Smoking should be prohibited in the data center;

(5) Data center personnel should be trained periodically ‘in firefighting -techniques and be assigned individual responsibilities in case of fire;

(6) Emergency procedures for handling minor and major fires should be prominently posted throughout the data center;

(7) Heat and smoke detectors should be installed in the ceiling, under raised floors and in the air ducts, alerting the, local fire department as well as internal personnel;

(8) Portable fire extinguishers should be located in strategic and accessible areas, be vividly marked, and periodically tested;

(9) Emergency exits and evacuation routes should be clearly labeled, and battery-powered emergency lights placed in strategic locations to assist in evacuation if the power should be interrupted;

(10) The computer center should be protected by an automatic fire suppression system;

(11) Emergency switches for cutting off power should be easily accessible near the data center exits;

(12) Emergency power shutdown should include the air conditioning system;

(13) Either the computer center should be equipped with temperature and humidity gauges that automatically activate warning signals if either moves outside the normal range, or personnel on duty should periodically check the temperature and humidity in the computer center and take appropriate actions as necessary;

[14) The computer center should be air conditioned by a separate system sufficiently protected from unauthorized access and made' from noncombustible materials;

(15) Air intakes should be protected against the introduction of noxious substances;

(16) Backup air conditioning should be available;

(17) The source of electric power should be sufficiently reliable to assure continued operations and be adequately protected from unauthorized access;

(18) The computer center should be backed up by an uninterruptible power source system;

(19) Procedures should exist and be applied for the retaining and/or copying of master files as a means of reconstructing a damaged or destroyed file;

(20) Sufficient generations of files should be maintained to facilitate reconstruction of records;

(21) At least one file generation should be kept at a location other than the file storage area;

(22) Copies of critical files, application programs, system software programs and critical documentation should be stored at an off-site location and be restricted from unauthorized access;

(23) Backup computer capacity should exist within the computer center and at an off-site location;

(24) Critical locations should be provided with the backup devices of terminals, modems, and communication lines;

(25) Backup arrangements should be documented and formally agreed upon by all parties concerned;

[26) A priority scheme should be established at the site and be approved by management, in the event that backup arrangements must be used;

(27) Backup procedures should be periodically tested;

(28) Off-site materials should be kept up-to-date;

3. System Software Controls. Control procedures concerning system software should be established and followed. Controls should ensure that the system software provides security and integrity of the system. A systematic procedure should be enacted to identify all potential system software programs that will satisfy organizational require’ments. A thorough cost and/or benefit analysis of system alternatives should be used to identify the most effective system. The software should be comprehensively tested prior to release for production. System software controls can be separated into the following categories.

Operating Systems.

System Utilities.

Program Library Systems.

File Maintenance Systems.

Data Communication Systems.

Data Base Management Systems.

System Software Change Controls.

Control techniques for each of these areas are detailed in the following sections:

a. Operating Systems Controls. Control procedures concerning operating systems- should ensure that a quality operating package is in place and is managed and operated correct ly. The following techniques should be considered to ensure proper controls over the operating system:

(1) A complete documented description of the operating system's design and operation should be provided by the vendor or developer;

(2) The operating system should prohibit one application program from accessing memory or data of another application program that is processing simultaneously;

(3) The operating system should prohibit an application program from accessing operating system instructions, password tables and other security algorithms;

(4) The operating system should prohibit operators from entering application data or changing users ' memory values at the computer console;

(5) The use of privileged instruction of the operating system should be strictly controlled;

(6) The operating system should control all input and/or output functions of data files ;

(7) Operating system instructions, password tables, and other authorization algorithms should be protected form unauthorized access when the computer system fails;

(8) The integrity of the operating system should be tested after initial installation;

(9) The operating system should prohibit application programs from overriding or bypassing errors that are detected during processing;

(10) All application programs or other system software should be run only when the operating system is operational;

(11) An audit trail of all operating system actions should be maintained either on the automatic console log or as part of the computer system' s job accounting data;

(12) The computer system's internal clock should be adequately protected from unauthorized access;

(13) The operating system should adequately and accurately schedule all jobs run on the computer system.

b. System Utilities Controls. Control procedures over system utilities should be established and controlled. The following techniques should-be considered to ensure proper controls over the sue and operation of system utilities:

(1) The vendor or developer of the system utilities should provide a complete documented description of their design and operation;

(2) A complete directory of all available utilities should exist;

(3) Computer operators should be denied access to system utility documentation;

(4) Management authorization should be required prior to the installation and use of new releases of utility programs;

(5) Controls that detect processing errors in system utilities should not be able to be overridden or bypassed;

(6) System utilities should not be able to be used to override or bypass controls within other system software or application programs.

c. Program Library Systems Controls. Control Procedures over program libraries should be established and followed. The following techniques should be considered to ensure controls over automated program libraries:

(1) A program library system should be used to “ control application programs;

(2) The vendor or developer of the program library system should provide a complete documented description of the system’s design and operation;

(3) The program library system should restrict access to application programs, control movement of programs from test to production modes, control movement of programs form source code to object code, and control changes to application programs;

(4) Program library system functions should be adequately supported by proper manual procedures;

(5) Control functions performed by the program library system should be protected so they cannot be bypassed;

(6) The program library system should provide an audit trail of all changes made to application programs; .

(7) The program library system should prevent the existence of more than one version of a source code and object code program;

(8) Obsolete programs should regularly be deleted from the source code and object code library;

(9) Computer operators should be denied access to all libraries maintained by the program library system.

d. File Maintenance Systems Controls. Control procedures covering file maintenance systems should be enacted and followed. Controls ensure that a quality file maintenance system is in place and properly used. The following techniques should be considered to ensure proper control over file maintenance systems:

(1) A file maintenance system should be used to control all disk and tape data set;

(2) The vendor or developer of the file maintenance system should provide a complete documented description of its design and operation;

(3) The file maintenance system should control the establishment, use, and retention of automated data files;

(4) File maintenance system functions should be adequately supported by proper manual procedures;

(5) Control functions performed by the file maintenance system should be protected so that they cannot be overridden or bypassed;

(6) The' file maintenance system should include redundancy controls, such as prohibiting more than one data file from having the same volume serial number;

(7) The file maintenance system should provide an audit trail of all uses and accesses of all automated data files.

e. Data Communications Systems Controls. Control procedures over data communications systems should be enacted and implemented. Controls should provide assurance against both illegal access and erroneous data transmission. The following techniques should be considered to control the operation and use of data communications systems:

(1) A data communications system should serve as the interface between terminals and the central data processing system;

[2) The vendor or developer of the data communications system should. provide a complete documented description of its design and operation;

(3) The data communications system should control access to and use of terminals, poll and receive messages from computer terminals or other computers, address and send messages back to computer terminals or other computers, edit and format input and output messages, handle error situations, reroute traffic when terminals or lines are inoperative, and Perform on-line formatting on visual display **terminals;**

(4) Data communications system functions should be adequately supported by proper documented procedures;

(5) Functions of the data communications system should be protected so that they cannot be overridden or bypassed;

(6) A built-in hardware identification code should be checked by the data communications system to ensure that no unauthorized terminals are being used;

(7) The data communications system should use a table of authorized terminal addresses to allow polling with the communications network;

(8) User authorization codes or passwords should be required by the data communications system to access the computer system and application programs; other system software and to enter transactions;

(9) Different authorization codes should be required to enter different types of transactions;

(10} The authorization code should identify the individual using the terminal and should be periodically changed;

(11) A nonprinting and/or nondisplaying facility should be used when keying in and acknowledging user authorization codes;

(12) A terminal identification check should be performed by the data communications system so that various transaction types can be limited to authorized data entry stations;

(13) The security matrix or table used to control access to the application system should be properly protected to prevent unauthorized access;

(14) A message header should be used by the data communications system to identify the source of the message, including proper terminal and use authorization code, message sequence number, including total number of message segments ,transportation type code and transportation authorization" code;

(15] This message header should be validated by the data communications system;

(16) The data communications system should include an end-of-transmission trailor that includes message and segment, value totals, including debits and credit s,. and an ending symbol;

(17) The data communications systems should reconcile counts and totals with header counts and totals;

(18) The data communications system should send acknowledgments to the terminal indicating receipt of messages and periodically test line and terminal operating status with standardized test messages and responses;

(19) The data communications system should use buffering to queue messages when a device, such as a terminal, is busy;

(20) The data communications system should maintain a transaction log of sequentially numbered and/or t ime-of -day-noted transactions;

(21) The transaction log should record the originating terminal, user authorization code, message identification, transaction type code, time of day that the transaction was logged, and transaction data;

(22) The transaction log should provide part of the audit trail, account for all error messages, and record, with control totals, all retrievals made by a particular terminal;

(23) All messages awaiting transmissions should be logged by the data communications system before being put into the transmission queue and then purged after transmission.

f. Data Base Management Systems Controls . Control procedures concerning data base management systems should be established and followed. Controls should provide assurance of the quality as well as the use of the DBMS. The following techniques should be considered to control the operation and use of data base management systems:

(1) Where appropriate, responsibility for administering the data base environment should be established at a high enough level to ensure independence;

(2) The vendor or developer of the data base management system should provide a complete documented description of its design and operation;

(3) The data base management system should provide security over data base accesses; control the addition, modification, and deletion of data; and provide a complete documented description of its design and operation;

(4) Integrity of data maintained within the data base should be ensured thorough utility programs that check the physical linkage of data within the database, control records that maintain interim balances of transactions and apply application programming standards that include procedures for maintaining integrity;

(5) Data base management system functions should be adequately supported by proper documented procedures;

(6) Functions of the data base management system should be protected so that they cannot be overridden or bypassed;

(7) The use of restricted instructions should be logged and checked periodically;

(8) The data base management system should use authorization codes or passwords to control access to data items;

(9) The data base management system should record unsuccessful attempts to access the data base;

(10) The data base management system should record which application programs have accessed each data item within the data base;

(11) The data base management system should prevent simultaneous updates to a record;

(12) The data base management system should prevent shared data from being deleted without consent of all users of the data;

(13) A log should indicate whether an application program has read, updated, created, or deleted a data item;

(14) All errors discovered by the data base management system should be logged for follow-up;

(15) Failures in the data base management system should be documented for supervisory review;

(16) A data dictionary should be developed and maintained, documenting the attributes of each data item and the security over each data item.

g. System Software Change Controls. Control procedures concerning system software changes should be established and followed. Controls should prevent unauthorized or inaccurate software changed. The following techniques should be considered to control system software changes:

(1) Formal documented system software change procedures should be established;

(2) Change request forms or other documentation should be used to originated system software modifications, with all forms sequentially numbered and accounted for;

(3) System software changes should be thoroughly tested to ensure that modifications function properly;

(4) System software modifications should be subjected to a system acceptance test before being placed in operations;

(5) All relevant documentation should be changed to reflect system software modifications;

(6) The volume of regularly scheduled system software modifications should be monitored and examined as an indicator of potential problems with the software, procedures or application;

(7) Computer operation personnel should have a list of system programmers to notify if the system software requires an emergency or immediate modification;

(8) Access to data files and application programs should be denied to the system programmer making a system software modification;

(9) The system programmer making an emergency modification should be denied access to data files and application programs that were operating when the problem occurred;

(10) The system programmer making an emergency system software modification should complete a signed statement

and leave it with the computer operator as to the encountered problem and its solution;

(11) Procedures should be established to ensure that emergency system software modifications are immediately subjected to a system acceptance test;

(12) Procedures should be established so that the accepted emergency modifications will be incorporated into the next operational version of the system software.

4. Hardware Controls. Hardware controls should be included by the manufacturer in the design of the computer equipment. Although computers possess a high degree of reliability, the potential for malfunction does exist. Hardware should be frequently checked to ensure that protection features are operating properly and have not been disabled. When equipment malfunctions, it should be recorded and reported to the vendor. An inventory of various features of all equipment should be kept, including location, model number, identification number, type and speed.Hardware controls should ensure the accuracy and reliability of computer processing. Although users and managers of ADP operations do not have much choice in this area, it is included for design or procurement considerations. Hardware control consist of:

- CPU Control.

- Peripheral Controls.

Data Communication Controls.

a. Central Processing Unit Controls. Controls should be built into the design of the control processing unit. Controls should ensure the accurate transmission of data and that only valid operation occurs. The following control techniques should exist within the CPU:

(1) Built-in parity bits should be used by the CPU to ensure that all data elements transmitted through the internal circuitry are correctly transmitted;

(2) Redundant character checking should be used by the CPU to insure the correctness of data processing;

(3) The CPU should use validity checks to ensure that only valid operation codes are used;

(4) The CPU should perform validity checks on the numbers used to access memory to insure that only valid numbers are used;

(5) The CPU should have automatic interlock controls to prevent the equipment from performing certain operations at the wrong time;

(6) Log should be maintained to record CPU meter readings at the start and end of each shift, and variances should be explained.

b. Peripherals Controls. Hardware controls should be built into peripherals to ensure the accurate transmission of data and the valid occurrence of operations. The following control techniques should exist within the peripherals:

(1) Parity checks of both individual and blocks of data should be made to ensure that all data elements are transmitted accurately;

(2) Validity check controls should be used to check the results of an operation with all possible valid solutions;

(3) Echo checks should be used to ensure that a transmitted command is actually performed or the data sent is correct;

(4) A read-after-write check should be used to ensure that the record just written was correctly recorded;

(5) Equipment diagnostic tests should exist for the computer to check if the equipment is functioning properly;

(6) With direct access storage devices, address comparisons should be made to verify the address to which data is to be written with the address called for by the instruction;

(7) Print synchronization controls should be used to check the timing of the printer to determine that print hammers of impact printers are activated at the moment when appropriate characters are in the correct position.

c. Data Communications Controls. Controls over data communication devices should be established and followed to ensure accuracy and privacy of transmitted data. The following control techniques should exist within data communication. devices:

(1) A unique hard-wired identification code, requiring no human intervention for its use, should be incorporated into each terminal device;

(2) The identification code should be checked and validated by the computer to ensure that no unauthorized terminals are being used;

(3) Data communications lines should be conditioned for improved accuracy and physical security;

(4) Scrambling or encryption techniques should be used in transmitting classified data;

(5) An automatic store-and-forward capability should be used to maintain control over messages queued for an inoperative or for a busy communications device;

(6) A message intercept function should be used to receive messages directed to inoperable or unauthorized terminals;

(7) parity checks should be used to detect errors in the transmission of data;

(8) Validity checks should be used to compare character so that erroneous data can be detected;

(9) Echo checking should be used to verify each character so that erroneous data can be detected;

(10) Forward error correcting techniques should be used for the detection and reporting of data communications errors using sophisticated redundancy codes;

(11) Techniques should be available for detecting erroneous retransmissions of data;

(12) Modems should be equipped with loop-back switches for fault isolation.

5. Distributed Processing and Network Operations Controls.

a. Control procedures concerning distributed processing and network operations should be formally established and followed. With the rapid increase of decentralization of systems and network operations, high risk areas of data security and integrity have become major concerns.

b. The following control techniques should be considered to ensure prop-er controls over distributed processing and network operations :

(1) The decision to undertake distributed processing should be documented and supported by cost and/or benefit analysis studies;

(2) The distributed processing requirements definitions should be responsive to management objectives in terms of the hardware configuration, data base configuration and hardware and communications network interface;

(3) A network implementation, conversion, and acceptance plan should be developed joint ly by systems and network user organizations and include user-prescribed test procedures and acceptance criteria;

(4) Users should participate in acceptance test, review test results, and provide approvals for functions over which they have jurisdiction;

(5) The operating provisions in the implementation plan should be consistent with the laws and regulations governing transmission of data within the country and/or internationally;

(6) Standards and policies for general network control should 'be clearly established and followed;

(7) Network standards and policies should be sufficiently broad-based, not to encumber local autonomy or operating objectives;

(8) As the general network capability is distributed, controls should be distributed to users;

(9) A network policy should require the ongoing identification of data set needing inter-system compatibility;

(10) A network should exist requiring audit trails and backup of all network communications activity for both network messages and application processed data;

(11) A network data review mechanism should be established to administer compatibility between system and data as the network grows;

(12) Hardware controls should include memory protection, alternate communication routing, communication protocols and timely failure recovery mechanisms ;

(13) Software controls over reentrant operating systems and current data base accesses and update should exist ;

(14) External labels should be used on cables, modems , control units, and other hardware devices to expedite fault isolation and service;

(15) Adequate controls and training regarding distributed data should exist to ensure data compatibility, integrity and effect ive data usage;

(16) Appropriate techniques and policies should be instituted for standardizing data definitions of shared data, maintaining common data dictionaries, and reconciling deviations . in data definition at remote facilities;

(17) Network data policies should require that data set ownership be clearly established;

(18) User and system responsibilities should be fully defined for coordinating and reconciling differences between distributed and/or replicated data bases prior to network implementation;

(19) Reconciliations should be able to be satisfactory performed under normal conditions, following network failures, and between varying application problems;

(20) Commonly shared and distributed data should be designed to readily permit integration and summarization at an organization-wide level to meet current or anticipated objectives;

(21) Network data standards should require and define data set change control procedures;

(22) Documentation and training should be provided to all network operations personnel;

(23) Adequate security should exist and be periodically reviewed over data controlled by network data base management systems and application and/or transaction processor, and over data handled at network processing facilities and remote locat ions;

(24) Review procedures for identifying and handling sensitive data should exist, and security classification for all levels of data sets in the network should be developed, consistent with information class if icat ion requirements;

(25) Procedures stating the preferred method for disposing of sensitive network documents at remote locations should exist and be communicated to the appropriate personnel;

(26) A central control function should be established to coordinate control reviews of network assets and resources at all network locations;

(27) Network asset inventories should be maintained at respective facilities and be periodically reviewed against actual network facilities;

(28) Control reviews should be used for assessing the ongoing integrity and overall control of the physical network;

(29) Summary control reports should be distributed to all network user organizations;

(30) Effective hardware and software backup provisions should exist for the entire network and for the individual facility;

(31) Adequate disaster and recovery procedures should be developed for each network processing facility; these procedures should be current and periodically tested;

(32) Written procedures should exist for switching to backup equipment, files, or systems;

(33) Network output requirements, operating schedules, processing procedures, and facility coordination policies should be fully established;

[34) Network availability and reporting, timing and/or response, storage, backup, and functional control requirements for all applications should be established by users and communicated to the responsible network operations organization;

(35) All network facilities should communicate with each other on a regular basis to discuss schedules and coordinate processing requirements and operating procedures;

(36) All network facilities should prepare schedules of consumable needs so that resources can be efficiently and effectively distributed throughout the network;

(37) Records should be maintained on the amount of resources used by each facility;

(38) All network locations should. receive regularly scheduled hardware prevent ive maintenance and log all hardware problems;

(39] Remote and local network control terminals, and operations personnel authorized to use them, should be identified;

(40) Policy agreements should exist for communications transmissions including provisions to effectively interface software applications and data bases among coordinated network facilities;

(41) Each network message and/or transmitted data unit should contain codes that identify the sender and intended receiver(s) ;

(42) All outgoing messages and/or data units should be edited for valid destination addresses;

[43) Communications provisions should exist to temporarily store messages and/or data units destined for remote facilities not in service. and for reactivating them when service is resumed;

(44) The assignment of transmission priorities should be consistent with established policy and appropriate for the need of the on-line application;

(45) All changes made to network operating systems software at remote processing facilities should be controlled by the central and/or main network processing facilities;

(46) Procedures should exist at remote facilities to ensure that all changes made to operating systems software are effectively controlled and made immediately visible to the control group directly responsible for the overall network;

(47) Proper access control should be maintained over the storage and use of network test equipment;

(48) Local and/or private communications lines and switches should be adequately secured and accessible only by authorized personnel;

(49) A cost and/or benefit analysis of encryption and private line acquisition should be made;

(50) When encryption is in use, the individual assigned the responsibility of management should not be involved with the operation or processing of data;

(51) Consolidated security reports should be periodically published reflecting recent network security reviews, and they should be available to all network user organizations;

[52) Remote users should have a list of standard terminal, modern, and controller device settings to facilitate problem determination;

(53) A comprehensive post-implementation technical review of the network should be required and performed by systems personnel;

(54) Local and consolidated network performance reports should be established to regularly report key elements such as network system availability, performance to schedules , response times, processing facility efficiencies and performance problems;

(S5) Adequate security measures should be in force at the backup facility.

D. APPLICATION CONTROLS

1. General.

a. Application controls are primarily concerned with data being processed. Collectively, they form a network of controls in a system to facilitate the production of accurate and reliable information. Certain internal control techniques should be incorporated directly into the applicat ions to help ensure accurate and reliable processing. Although these control techniques may be unique to a particular applications, they can normally be grouped according to various stages of data processing. The basic application control techniques consist of:

System Design, Development and Modification Controls;

Data Origination Controls;

Data Input Controls;

Data Process ing Controls;

Data Output Controls;

b. The specific control techniques for each of these five components are detailed in this section. It should be noted that many techniques apply to more than one component ; thus , this section should be referred to in its entirety to ensure coverage of all appropriate techniques.

2. System Design, Development , and Modification Controls. The adequacy and effectiveness of controls in computer-based systems begins with the methods and procedures used during the system development process. Procedures should require a structured design, development , and modification process that provides adequate separation of duties and assures user, management, and internal auditor participation. Additional key elements are adequate documentation, effective computer program testing, effective system acceptance testing, and effective computer program change control procedures.

a. Systems Development Methodology Controls. Systems development should be predicated on life-cycle management (LCM) concepts and procedures. This technique is as applicable during initial system design as it is during the modification process; thus , appropriate elements of the LCM should be utilized whenever system changes are made. LCM is particularly advantageous because it promotes effective communication among programmers, systems analysts , acceptance testers, users, internal auditors, and management personnel.

The following techniques should be considered to properly control systems development:

(1) A formal management controlled approach for system development should exist;

(2) The system development process should include:

- Feasibility study.
- User need definition.
- Conceptual system design.
- Cost and/or benefit analysis.
- Detailed system analysis and design.
- Programming.
- Testing.
- Procedure preparation.
- Conversion.
- System acceptance.
- ADP Systems Security Office (ADPSSO) review and certification of protection specifications.
- Operations.
- Post-implementation audit.

(3) Formal requests for new or revised systems should be prepared by users submitted with proper authorization and used to develop the conceptual system design;

(4) The conceptual system design should be used to determine the technical and operational feasibility of the system;

(5) A cost and/or benefit analysis should be performed to ensure that the conceptual system will produce desired results economically;

(6) Additional hardware and system software requirements should be consistent with ADP plans and be included in the cost and/or benefit analysis, and be used to prepare the computer programs;

(7) The detailed system design should be consistent with the conceptual design, be based on the feasibility study and on the cost and/or benefit analysis, and be used to prepare the computer programs;

(8) Upon completion of all programming, each program, interrelated subsystem and the entire system should be thoroughly tested;

(9) Program and system test results should be reviewed and signed by the system analyst;

(10) Program and system test results should be reviewed by the ADP Systems Security Officer and certified that the system meets documented and approved system protection specifications;

(11) Procedures should exist to ensure that no data is lost or erroneously changed during conversion to the newly designed system;

(12) Sufficient computer time should be allocated for the conversion process;

(13) Prior to acceptance testing, the newly designed system should be tested in parallel operations with the old system;

(14) The system should be "acceptance tested" by a group independent of the programmers and analysts who designed the system to ensure that it performs in accordance with specifications and meets user needs;

(15) The system acceptance group should certify in writing that the system performs in accordance with all functional and performance specifications;

(16) This group should control all changes to the system to maintain its integrity on a continuing basis;

(17) System implementation should be coordinated with all personnel involved and other systems affected;

(18) A post-implementation audit of the entire system, manual and automated, should be performed by the internal audit staff after the system has been in operation for several months;

(19) The LCM concepts and procedures should be reviewed to assess whether they reflect current techniques and procedures applied in the ADP community;

(20) The following personnel should be involved in the system development process: project managers, users, system

analysts, programmers, records managers, acceptance testers and internal auditors;

(21) The duties of the personnel on the development project should be clearly separated;

(22) Specific tasks and timeframes for completing the tasks should be established for each member of the development project;

(23) The project manager should be authorized to make decisions on personnel resources, scheduling and most technical project matters;

(24) Adequate resources should be provided to successfully complete the system development project;

(25) A management project steering committee should be formed to oversee and review progress throughout the life-cycle;

(26] Users should actively participate in system development;

(27) The user should be the final authority on whether the system meets its intended purpose and should accept the system in writing.

b. System Reporting Documentation Controls. The objectives of documentation is to provide a clear, understandable description of the system. Good documentation increases the ease and accuracy of computer program maintenance and provides the basis for evaluating internal controls in the system. The following control techniques should be considered to ensure adequate system documentation:

(1) Ensure that programmers implement established standards for documenting different data processing functions;

(2) A project request document should be prepared to provide the means for a user to request the development, procurement, or modification of software or other ADP-related services;

(3) For significant system additions or modifications, a feasibility study document should be prepared to provide an analysis of the objectives, requirements and system concepts, an evaluation of alternative approaches, and an identification of a proposed approach;

(4) A cost and/or benefit analysis document should be prepared to give managers, users, designers, and auditors adequate information to evaluate alternative approaches for significant system additions or modifications;

(5) A functional requirements document should be prepared to provide the basic understanding between users and designers of the system;

(6) A data requirements document should be prepared to provide a data description and technical information about data collection requirements;

(7) Detailed system and/or subsystem specifications should be developed;

(8) Detailed program specifications should be developed for all programs of the system;

(9) Detailed specifications should be developed for data bases used by the system;

(10) A users or procedures manual should be developed to document the functions of the system;

(11) An operations manual should "be developed to describe the system and its operational environment for computer operations personnel;

(12) Program and system documentation should be accessible to computer operat ions personnel;

(13) A program maintenance manual should be developed to give the maintenance programmer sufficient information to understand the programs , their operating environment, and their maintenance procedures;

(14) A plan should be documented to test the system;

(15) A test analysis report should be developed to document the test analysis results and findings;

(16) All documentation should be periodically reviewed to ensure that it is current and complete and adheres to established standards;

(17) Copies of all documentation should be stored off the premises;

(18) There should be signatures or other documented evidence of who performed systems and programming work;

(19) Documented procedures should exist for controlling all system documentation.

C. <u>Program Testing and System Acceptance Controls</u>

(1) Programs that make up a computer-based application should be thoroughly tested to assure accurate and reliable processing. Since programming errors can be made in either the symbolic language or program logic, error checking should be performed at several different stages in program development.

(2) The system acceptance process is the last line of defense against implementing an application with major errors. It serves as a "detective" control over the preceding phases of the development project. It gives users, internal auditors, designers, implementers, and other concerned parties an opportunity to view the system in final form before it becomes operational. If satisfied with results of the system acceptance process, acceptance testers should certify its accuracy and completeness in writing.

(3) The following control techniques should be considered to properly control program testing and system acceptance. It should be noted that current technology is addressing the automation of some of these controls.

(a) All computer programs should be checked by the programmer and his/her supervisor through desks checks or walk-throughs before program assembly or compilation;

(b) All computer programs should be reviewed after assembly or compilation to ensure that errors disclosed by these routines are corrected;

(c) Each program, subsystem, and then the entire system should be tested;

(d) Test data should be treated like live data, as opposed to entering codes in the test data to indicate that it is not normal production data.

(e) System acceptance should be performed using test data similar to, but independent of, program testing data;

(f) System acceptance transactions should be tested like live transactions, as opposed to having special codes entered in the transaction to indicate that it is not normal production data;

(g) Sufficient volumes of test and system acceptance transactions that have a wide range of valid and invalid conditions should be entered and processed;

(h) Sufficient time should be allocated for thorough testing and system acceptance purposes;

(i) Sufficient staff members should be allocated for testing and system acceptance purposes;

(j) Test cases and system acceptance test transactions should be developed to review:

Mainline and end-of-job logic.

Each rout ine.

Each exception.

Abnormal end-of-job conditions.

Combinations of parameter cards and switch settings

Unusual mixtures and sequences of data.

Control features; e.g. , salary parameters

(k) Test and system acceptance data should include cases that test for the following:

Codes.

Characters.

Fields.

Combination of fields.

Transactions.

Calculations.

Missing data.

Extraneous data.

Amounts.

Units.

Composition.

Logic decisions .

Limit or reasonable checks .

Sign.

Record matches.

Record mismatches.

- Sequence.

Check digit.

Crossfooting of quantitative data.

Control totals.

(1) Programming and software packages should be used to improve computer programs' efficiency and effectiveness;

(m) New programs should be run parallel to old ones to help assure their accuracy;

(n) All computer-based systems should be subjected to a system acceptance process;

(o) The system acceptance should evaluate whether the entire system, both manual and automated processes, is performing in accordance with system specifications and processing standards;

(p) System acceptance should be performed by individuals independent of those who performed the analysis, design, and/or development of the system;

(q) Once system acceptance has been completed, a written certification that the entire system performs in accordance with all functional and performance specifications should be required before the system is placed in operation.

d. Program Change Controls. Control procedures for computer program changes should be established and followed. The intent of these controls is to prevent unauthorized, inaccurate, and unreliable program changes from being incorporated into the live production environment . Both scheduled and emergency changes need to be appropriately controlled to maintain the continued integrity of a computer-based system. The following control techniques should be considered to ensure that proper controls are being maintained over computer program changes:

(1) Formally -approved written standards for program changes and documentation should exist and be followed;

(2) Procedures defining who can initiate and who can authorize change requests should be established;

(3) Change requests should be written, including a description of the nature of and reasons for the proposed change as well as security and privacy specifications;

(4) Change requests should be made by users on sequentially numbered forms;

(5) User authorization and written approval should be required for all program changes;

(6) ADP proj ect management authorization and written approval should 'be requir-ed for all program changes;

(7) Changes should be approved by individuals who do not operate the computer, except for microcomputers;

(8) Procedures should exist to ensure that all program changes, both scheduled and emergency, are subjected to the testing and acceptance process;

(9) Application changes should be tested prior to operational use;

(10) Modified programs should be tested under normal operating conditions;

(11) Users should be involved in preparing test data and reviewing test results;

(12) Test results should be reviewed with supervisory personnel before revisions become effective;

(13) All errors detected during the conversion process should be investigated before and after correction;

(14) Certification should be made that test results demonstrate adequate protection from fraud, waste, and misuse of the program;

(15) All program changes should be documented, and appropriate program, system, operations, and user documentation should be updated as changes are made;

(16) A log should be maintained of all completed changes and all changes in progress;

(17) Program changes should be documented by individuals who do n-et opera t-e the computer;

(18) Certification should be made that documentation specifications are met;

(19) Program library software should be used to report all changes to ADP managers and to users;

(20) Endurances should be made that changes meet users' needs;

(21) Procedures should exist to determine if any other system if affected by the program modification;

(22) Original programs should be retained until changes have been processed and new programs tested and updated;

(23) Once modifications have been implemented, procedures should prevent original programs from being used by mistake;

{24) Procedures should be in place to ensure that an "abnormal" volume of regularly scheduled program modifications results in a review to determine if a problem exists with programs, procedures, or the computer-based system;

(25) A limit should be placed on the frequency of program changes, except for emergency changes;

(26) When emergency changes are made, both the user and ADP project manager should be notified;

(27) All problems related to program changes should be documented and given to the ADP project manager.

3. Data Origination Controls

a. Data origination controls are used to ensure the accuracy, completeness and timeliness of data prior to its being converted into machine-readable format and entered into the computer application. Controls over the data should be established as close to the point of origination as possible , as the remainder of the application processing depends upon the accuracy of source data. Additionally, controls should be maintained throughout this manual process to ensure that the data reaches the computer application without loss , unauthorized addition or modification, or other error.

b. The following control techniques should be considered to ensure that controls are being maintained over data origination:

(1) Documented procedures should exist to explain the methods for proper source document origination, authorization, data collection, input preparation, and error handling retention;

(2) Duties should be separated to ensure that no one individual performs more than one of the following: originating data, entering data, processing data, or distributing output;

[3) When beneficial, forms (either paper or electronic) may be used to record initial data in a uniform format;

(4) Source documents should be designed in such a manner as to minimize errors and omissions and to ensure data uniformity;

(5) Source documents should be prenumbered if accountability is a requirement ;

(6) For each type of transaction, the source document should provide a unique identifying code;

(7) Each transaction should have a cross-reference number that can be used to trace data to and from the source document;

(8) Access to source documents, blank input forms and copies of source documents should be re-stricted to authorized personnel only;

(9) Authorizing signatures should be used for all paper transactions, when required;

(10) Duties should be separated within the user organization to ensure, unless authorized, that one individual does not prepare more than one type of transaction;

(11) Blank source documents should be stored in a secure location;

(12) Duties should be separated within the user organization to ensure that no one individual performs more than one of the following: originating the source document , authorizing the source document, or controlling the source document;

(13) The user organization should have a control group responsible for collecting and completing source documents;

(14) This control group should verify that source documents are complete and accurate. Furthermore, all documents should be accounted for, transmitted in a timely manner and authorized;

(15) A separate user group should perform the input function when the user organizationis responsible for its own data entry;

(16) When transmitted for conversion, source documents should be transported in accordance with their security classifications;

(17) Documented procedures should exist to explain the methods for source document error detect ion, correct ion and reentry; ‘

(18) The control group should identify errors to facilitate the timely correction of erroneous information;

(19) Error logs should be used to ensure timely follow-up and correction of unresolved errors;

(20) Originators of source documents should be notified by the control group of all error;

(21) Source documents should be retained as a safeguard against data loss or destruction during subsequent processing;

(22) Source documents should have specific retention periods;

(23) Source documents should be stored in a logical manner to facilitate retrieval;

(24] Whenever a source document leaves the originating organization, a copy should be kept in the organization;

(25) When reaching their expiration dates, source documents should be removed from storage and destroyed in accordance with the approved disposal schedule.

4. Data Input Controls

a. Data input controls ensure the accuracy, completeness and timeliness of data during its conversion into machine-readable format and entry into the applicat ion. Data can be entered through either on-line or batch processing. As there is a large degree of overlap between the control techniques for these two processes, no distinction is made in the following techniques indicating whether they apply to on-line, batch, or both.

b. The following control techniques should be considered to ensure that proper controls are being maintained over data input:

(1) Documented procedures should exist to explain the methods for data conversion and entry;

(2) Data entry terminal devices should be locked in a physically secure room;

(3) The work entered on a terminal should be restricted by the authority level assigned to each terminal;

(4) Password controls should be used to prevent unauthorized use of terminals;

(5) When keying passwords and authorization codes, non-printing and nondisplaying facilities should be used;

(6) An immediate report should be produced of unauthorized attempts to access the system via terminals;

(7) Management should review unauthorized usage reports;

(8) Each individual user of the on-line system should be limited to certain types of transactions;

(9) Individual passwords should be changed periodically;

(10) Passwords should be deleted once an individual changes his or her job function or level of access;

(11) Management should periodically review the propriety of the terminal authority levels;

(12) Terminal hardware features should include the following:

(a) Built-in terminal identifications that automatically validate proper terminal author izat ion,

(b) Terminal logs that are automatically data and time stamped for logging purposes, and

(c) Record counts that are automatically accumulated for logging purposes;

(13) Parity checking should be used to check each character and each message;

(14) Documented procedures should exist to explain the process of identifying, correcting and reprocessing data rejected by the application;

(15) Error messages should promptly be displayed with clearly understood corrective actions for each type of error;

(16) All data that does not meet edit requirements should be rejected from further processing by the application, produce an error message and be written on an automated suspense file;

(17) The suspense file should include the data and time a transaction was entered along with the identity of the user who originated the transaction;

(18) Suspense file processing should create record counts and predetermined control totals;

[19) Valid correction transaction should purge the automated suspense file of corresponding rejected transactions;

(20) All corrections should be reviewed and approved by supervisors before reentry;

(21) Procedures for processing corrected transactions should be the same as those for processing original transactions, except for the supervisory review and approval;

(22) The ultimate responsibility for the completeness and accuracy of all application processing should remain with the user;

(23) The terminal user should correct errors caused by data conversion or entry;

(24) The user originating the transaction should correct errors not caused by data conversion or entry;

(25) The suspense file should be used to control follow-up, correction, and reentry of rejected transactions;

(26) The suspense file should periodically be analyzed to determine whether too many errors are being made and whether corrections are being processed in a timely manner;

(27) Debit and/or credit entries, rather than delete or erase commands, should be used to correct errors on the suspense file;

(28) Record counts and predetermined control totals should be appropriately adjusted by correcting transactions;

(29) Intelligent" terminals should be used to allow front-end validation, editing, and control;

(30) Data validation and editing should be performed as early as possible in the data flow to ensure that the application rejects any incorrect transaction before its entry into the system;

(31) preprogrammed keying formats should be used to make sure that data is recorded in the proper field, format, etc. ;

(32) Computer-aided instruction, such as prompting, should be used with on-line dialogue to reduce the number of operator errors;

(33) Batch control totals, record counts, and predetermined control totals submitted by the data processing control group should be used by the computer-based system to validate the completeness of data input into the application;

(34) No personnel should be able to bypass validation and editing problems;

(35) Data validation and editing should be performed for all input data fields;

(36) All documents entered into the application should be signed or marked in some way to prevent accidental duplication or reuse of the data;

(37) The data processing organization should have a schedule by application showing when data requiring conversion and when data requiring entry will be received and needs to be completed;

(38) Input document should be retained in a manner that enables tracing them to related originating documents and output records;

(39) All converted documents and input documents returned to the data processing control group should be logged in and accounted for;

(40) The data processing organization should have a control group responsible for data conversion and entry of all source documents received from users;

(41) This group should account for all batches of source documents received from the user to ensure that no batches have been added or lost;

(42) This group should independently develop record counts and predetermined control totals to be balanced with those of the control group in the user organization, and all discrepancies should be reconciled.

5. Data Processing Controls

a. Data processing controls are used to ensure the accuracy, completeness, and timeliness of data during processing by the computer. These controls apply to application programs and computer operations related to a given application. Data processing is usually accomplished in either batch or real time. As with data input controls, no distinction is made in the listing of the data processing control techniques for batch versus real time.

b. The following techniques should be considered to ensure that proper controls are being maintained over data processing. Several of the techniques listed previously in this section, particularly those relating to editing and error handling, are applicable to data processing as well. The reader should refer back as the following techniques are considered:

(1) Documented procedures should exist to explain the methods for proper data processing of each application program;

(2) Operator instructions should include system start-up procedures, backup assignments, emergency procedures, system shutdown procedures, error message debugging instructions and system and job status reporting instructions;

(3) Application programs should be prevented from accepting data from computer consoles;

(4) The system should have a history log that is printed on both a line printer and the console;

(5) The log should routinely be reviewed by supervisors to determine the cause of problems and the appropriateness of actions taken;

(6) The data processing organization should have a schedule showing when each application program is to be run and needs to be completed;

(7) The data processing organization should have a control group responsible for controlling all data processing operations;

(8) Each input transaction should have a unique identifying transaction code that directs it to the proper application program for processing;

(9) Standardized default options should be built into the program logic;

(10) Computer generated control totals (run-to-run totals) should automatically be reconciled to check for completeness of processing;

(11) Controls should be in place to prevent operator from circumventing file checking routines;

(12) Controls should ensure that output counts equal input counts;

(13) All programs that include a table of values should have an associated control mechanism to ensure accuracy of the table value;

(14) There should be an audit trail in the application to assist in reconstructing data files;

(15) Messages and data should be able to be traced back to the user or to the point of origin;

(16) The application should prevent concurrent file updates;

(17) Transactions should be dated and time-stamped for logging purposes;

(18) There should be control to verify that proper data is used when computerized data is entered into the computer application;

(19) When computerized files are entered into the computer application, there should be controls to verify that the proper version of the file is used;

(20) Application programs should include routines for checking internal file header labels before processing;

(21) Internal trailer labels should contain control totals to provide a check that all records are on the file;

(22) File completion checks. should be performed to ensure that application files have been completely processed, including both transaction and master files;

(23) Record and predetermined control totals generated by the application should be used by the data processing control group to validate the completeness of data processed by the system;

(24) A direct update to files should cause creation of a record added to a backup file and recording of the transaction on the transaction history file;

(25] A “before and after picture” of the master file being updated should be maintained;

(26) Relationship editing should be performed between the input transaction and master files to check for appropriateness and corrections prior to updating;

(27) The data processing control group should balance batch counts, record counts, and predetermined control totals of data submitted for processing; ensure that input and/or work and/or output files used in computer processing are correct and maintained in logs; and ensure that restarts are properly performed.

6. <u>Data Output Controls.</u> Data output controls are used to ensure the integrity of output and the correct and timely distribution of outputs produced. Not only must outputs be accurate, but they must also be received by users in a timely and consistent manner. Of critical importance is the interface between the data processing organization and the user department. Outputs can be produced either in a batch mode or on-line. Again, as there is a large degree of overlap in the control techniques for these two methods, no distinction is made within the specific techniques.

a. Documented procedures should exist to explain the methods for proper balancing and reconciliation of output products;

b. The data processing organization should have a control group that is responsible for reviewing all outputs produced by the application;

c. This group should monitor the processing flow to ensure that programs are process according to schedule;

d. This group should review output products for general acceptability and completeness;

e. This group should reconcile each output batch total, record count and predetermined control total with input batch totals, record counts and predetermined control totals before releasing any reports in order to ensure that no data was added or lost during processing;

f. System output logs should be kept to provide an audit trail for the outputs and to summarize the number of reports generated, the number of copies of each report, the recipients of each report and the report security status;

g. These logs should be reviewed by supervisors to determine the correctness of output production;

h. A transaction log kept by the application should be compared regularly with a transmission log kept at each output device to ensure that all transactions have been properly processed to the final output steps;

i. Transactions should be able to be traced forward to the final outputs and backward to the original source documents ;

j. The user should have a control group that is responsible for reviewing all output received from the data processing organization;

k. This group should be given lists of all changes to the application master file-data and programmed data. of all internally generated transactions produced by the application, of all interface transactions processed by the application, and of all transactions entered into the application;

1. This group should use these lists to verify the accuracy and completeness of all output;

m. This group should verify all computer-generated batch totals, record counts and predetermined control totals with its own manually developed batch totals, record counts, and predetermined control totals;

no Documented procedures should exist to explain the methods for proper handling and distribution of output reports;

o. userers should periodically be questioned to determine whether they find the reports they receive relevant; whether they find the data presented on reports accurate, reliable and useful; whether they should be removed form or added to distribution lists for receiving reports; and whether they have suggestions concerning the format, content, frequency, and timeliness of reports they receive;

p. The user should retain ultimate responsibility for the accuracy of all outputs;

q. The cover sheet of every report should clearly identify the recipients' names and locations;

r. A priority system should exist to ensure that critical outputs are produced on time;

E. MICROCOMPUTER CONTROLS. Control procedures over microcomputer acquisition and operation should be established and followed to ensure the proper use of microcomputers and the accuracy of the processed data. Implementing certain control procedures unique to microcomputers should decrease the risk of illegal system access, data loss, and stolen hardware. Internal control techniques enumerated elsewhere in this Guideline may also apply to microcomputer. The reader should refer to the techniques detailed under Management Controls, Operations Controls, and Application Controls to ensure control over microcomputer operation. The following techniques should be considered to ensure that proper controls exist in the microcomputer environment:

1. ADP and user management should establish and document microcomputer acquisition policies, criteria, and procedures within an approved organizational statement of strategy;

2. Acquisition should be justified in terms of objectives and benefits to be realized, and the level of detail in the justification documentation-should be kept to a minimum, commensurate with need and judicious management practices;

3. Management should be established allowing only authorized personnel use of microcomputer resources to protect the data, software, and physical equipment from improper use or theft;

4. Policies should be established allowing only authorized personnel use of microcomputer resources to protect the data, software, and physical equipment from improper use or theft;

5. Requisition, approval, and subsequent placement of microcomputers should be documented;

6. Written guidelines should exist on develop-or-buy alternatives for application software;

7. Personnel with appropriate backgrounds should be designated to develop application software and/or to evaluate application software packages offered by vendors.

8. Procedures should exist to allow user groups to accept application software developed internally;

9. User groups should be required to provide program documentation for approval prior to using application software developed by the group;

10. Management approval and user group concurrence should be secured in instances when data processing personnel modify application software packages;

11. Management approval should be secured before application software packages are modified by user groups;

12. A procedures manual should be developed to document the functions and capabilities of microcomputer-based systems;

13. Procedures related to sharing application programs and data should be established;

14. A central depository of documentation of programs under development should be kept to prevent duplication of effort;

15. Proprietary software packages should be protected against copying or modification;

16. A formal document should state that copyright laws will be rigidly enforced;

17. Hard disks should be backed up onto another storage medium on a regular basis;

18. When microcomputers. are approved to access data in other computer facilities, procedures that adhere to policy concerning the creation and maintenance of data files on these microcomputers would be specified;

19. When microcomputers are approved to access data in other computer facilities, procedures that adhere to policy concerning gaining access to microcomputers and other computer resources accessible to these microcomputers should be established;

20. Codes, passwords, or other devices should be used to identify authorized users of the microcomputers;

21. When microcomputers are approved to access data in the organization's other computer facilities, usage on these microcomputers, including user identification, level of resource access, and all transactions introduced for processing should be logged by the other facilities;

22. When they are away from the microcomputer area, users of sensitive data should securely lock up all diskettes;

23. Rooms in which microcomputers are located should be secured after normal working hours;

24. Microcomputers should be stored in a controlled area;

25. Property management procedures concerning microcomputer components should be followed, including marking-them with unique identification numbers and recording and securely storing all identification numbers, serial numbers, and equipment descriptions.